COMNAVRESFOR INSTRUCTION 5300.5B

From: Commander, Navy Reserve Force

Subj: INFORMATION TECHNOLOGY AND NAVY MARINE CORPS INTRANET GUIDANCE

Ref: See appendix c.

Encl: (1) Administrative Information Technology Procedures for the Navy Reserve Force

1. Purpose. The purpose of this instruction is to promulgate guidance for Navy Reserve Information Technology (IT) usage to meet claimancy-wide requirements. These requirements maximize efficiency and cost effectiveness for Enterprise Architecture (EA), Information Assurance (IA), cybersecurity, security, management, distribution, and administration and user responsibilities, per references (a) through (y), within a limited Navy Marine Corps Intranet (NMCI)/Continuity of Service Contract (CoSC) budget. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. COMNAVRESFORINST 5300.5A.

3. Scope. This instruction provides policy for the administration of the Navy Reserve Force’s IT investments and IT services portfolio.

4. Due to the rapid pace and evolving nature of IT and related systems, in addition to this document, users shall reference the Commander, Navy Reserve Forces Command (COMNAVRESFORCOM) (N6) SharePoint page for further clarification, guidance, and updates to policy.

5. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of January 2012.

6. Review and Effective Date. Per OPNAVINST 5215.17A, COMNAVRESFORCOM will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 10 years after effective date unless reissued or canceled prior to the 10-year anniversary date, or an extension has been granted.

T. W. LUSCHER
Deputy

Relesability and distribution:
This instruction is cleared for public release and is available electronically only via COMNAVRESFORCOM Web site https://www.mynrh.navy.mil/
ADMINISTRATIVE INFORMATION TECHNOLOGY PROCEDURES FOR THE NAVY RESERVE FORCE
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CHAPTER 1</strong></td>
<td></td>
</tr>
<tr>
<td>NMCI and NETWORK SERVICES</td>
<td>1-1</td>
</tr>
<tr>
<td>NMCI Account Management</td>
<td>1-1</td>
</tr>
<tr>
<td>SIPRNET Accounts and Tokens</td>
<td>1-2</td>
</tr>
<tr>
<td>Account and Token Association</td>
<td>1-3</td>
</tr>
<tr>
<td>System Authorization Access Request (SAAR-N)</td>
<td>1-4</td>
</tr>
<tr>
<td>Other Accounts: Defense Enrollment and Eligibility Reporting System (DEERS)/Real-time Automated Personnel Identification System (RAPIDS)</td>
<td>1-4</td>
</tr>
<tr>
<td>Government-Furnished Equipment (GFE) phones, MobiKEY, and Mobile Cellular Data Device (MCDD)/Wi-Fi</td>
<td>1-4</td>
</tr>
<tr>
<td>Navy Reserve Force, NAVOPSPTCEN Wi-Fi (NNWF)</td>
<td>1-5</td>
</tr>
<tr>
<td>Ready 2 Serve (R2S)</td>
<td>1-5</td>
</tr>
<tr>
<td>Message Traffic</td>
<td>1-5</td>
</tr>
<tr>
<td>COMNAVRESFOR Customer Support Center (CSC)</td>
<td>1-5</td>
</tr>
<tr>
<td><strong>CHAPTER 2</strong></td>
<td></td>
</tr>
<tr>
<td>FACILITIES AND BUDGET</td>
<td>2-1</td>
</tr>
<tr>
<td>NIPRNET Assets</td>
<td>2-1</td>
</tr>
<tr>
<td>SIPRNET Assets</td>
<td>2-2</td>
</tr>
<tr>
<td>Desktop Phones</td>
<td>2-2</td>
</tr>
<tr>
<td>Printing Services</td>
<td>2-2</td>
</tr>
<tr>
<td>DEERS/RAPIDS Terminals</td>
<td>2-3</td>
</tr>
<tr>
<td>Secure Space Certification</td>
<td>2-3</td>
</tr>
<tr>
<td>Military Construction (MILCON) and Facility Restoration</td>
<td>2-4</td>
</tr>
<tr>
<td>Subject</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>MANAGEMENT RESPONSIBILITIES</td>
<td>3-1</td>
</tr>
<tr>
<td>Introduction</td>
<td>3-1</td>
</tr>
<tr>
<td>System Change Requests</td>
<td>3-1</td>
</tr>
<tr>
<td>Information Technology (IT) Inventory</td>
<td>3-2</td>
</tr>
<tr>
<td>NMCI Pre-Invoices (non-NMCI IT) Procurement Requests</td>
<td>3-2</td>
</tr>
<tr>
<td>NMCI Services Request (6AG)/ Requirement to Award Process Tool (RAPT)</td>
<td>3-2</td>
</tr>
<tr>
<td>Infrastructure Account Management Information System Security Manager</td>
<td>3-3</td>
</tr>
<tr>
<td>ISSMs/ISSOs Responsibilities</td>
<td>3-3</td>
</tr>
<tr>
<td>SARR-N Forms</td>
<td>3-5</td>
</tr>
<tr>
<td>Key Management Infrastructure (KMI)</td>
<td>3-5</td>
</tr>
<tr>
<td>Collaboration Tool: SharePoint (NRH)</td>
<td>3-6</td>
</tr>
<tr>
<td>Collaboration Tool: Defense Collaboration Services (DCS)</td>
<td>3-9</td>
</tr>
<tr>
<td>NNWF Usage Procedures and User Responsibilities</td>
<td>3-9</td>
</tr>
<tr>
<td>Cybersecurity Workforce (CSWF)</td>
<td>3-13</td>
</tr>
<tr>
<td>User Training</td>
<td>3-14</td>
</tr>
<tr>
<td>Continuity of Operations Plan (COOP)</td>
<td>3-15</td>
</tr>
<tr>
<td>DEERS/RAPIDS</td>
<td>3-15</td>
</tr>
<tr>
<td>Outlook Web Access (OWA)</td>
<td>3-15</td>
</tr>
<tr>
<td>Common Access Card (CAC) Readers</td>
<td>3-15</td>
</tr>
</tbody>
</table>
CHAPTER 1
NAVY MARINE CORPS INTRANET (NMCI) AND NETWORK SERVICES

1. NMCI Account Management

a. Active NMCI unclassified accounts are required for all members of the Navy Reserve, including Full-Time Support (FTS), Selected Reserve (SELRES), and Volunteer Training Unit members. Active NMCI unclassified accounts are also required for all government civilian employees under the responsibility of Commander, Navy Reserve Force (COMNAVRESFOR) and may be required for some contractors who are under contract with COMNAVRESFOR or any of its subordinate commands. A profile for every account will be established in NMCI Enterprise Tool (NET), which will allow COMNAVRESFOR to maintain an accurate accounting of the number of accounts assigned to COMNAVRESFOR at any given time.

b. An account shall be deactivated upon the death, retirement, separation of a service member, civilian employee, or contractor. The respective Assistant Customer Technical Representative (ACTR) may choose temporary suspension or permanent deactivation. The Customer Technical Representative (CTR) may temporarily suspend an account if the service member intends to join the Navy in another capacity (FTS to SELRES or contractor, etc). The account should be permanently deactivated if the member has not transferred after the 90 day period has expired.

c. The existing account should be reactivated for members transferring from a non-NMCI command and for those returning to a command with NMCI access. New accounts should not be created if an account already exists in the NMCI active directory.

d. Personnel with NMCI accounts should login within required periodicities as determined by Commander, Naval Network Warfare Command (COMNAVNETWARCOM) to ensure their account is not disabled or deleted. Non-Classified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) accounts are currently disabled after 60 days of dormancy and deleted after 90 days of dormancy (30 days after disablement) for all military, civilian, or contractor personnel who fall under the responsibility of COMNAVRESFOR. However, this policy may change pursuant to COMNAVNETWARCOM guidance. Contact Commander, Navy Reserve Forces Command (COMNAVRESFORCOM) (N6) or check the COMNAVRESFORCOM (N64) Navy Reserve Homeport for the most current policy. In order to avoid deletion for mobilizing members, units should request a deployed status through COMNAVNETWARCOM’s Individual Augmentees (IA) watch or access management team or use the Deployment Management Tool (DMT).

e. Account Definitions

(1) Active Account: Provides the member access to the NMCI Network, e-mail, and personal storage space (H: Drive).
(2) Deactivated Account: End of service for an NMCI Account. This occurs when all NMCI services are discontinued. The account will be moved out of the local command Organizational Unit (OU) structure, attributes will be reduced to digital identity, flat name space, and associated data will be compressed and moved to a permanent data storage facility. Do not deactivate the accounts of members who are transferring between commands that are serviced by NMCI.

(3) Disabled/Suspend Account: An account that is not accessible and all e-mail are rejected. This type of account would be used by the information system security manager to lock an account.

(4) Reactivated Account: A deactivated account reestablished with stored digital identity.

2. SIPRNET Accounts and Tokens

a. Navy Reserve Force service members, government civilians and contractors within the Navy Reserve Force use the terms “SIPR account” and “SIPR token” interchangeably. This has caused confusion for our total force members and SIPR account providers/facilitators. For clarification, an account is the actual requested, assigned, and provided permission for a total force member to access electronic/networked SIPR media. A token is the physical piece of hardware (an access card) required for authentication to access an account.

b. Not all Navy Reserve Total Force Members qualify for SIPR access. However, if a member has been identified as having a need to know, and has the requisite clearance then a request for a NMCI SIPR account may be submitted. Requests must be made with a completed System Authorization Access Request (SAAR-N) form along with a DD-2842 (08-09) and identification (2 forms of ID are required for non-military). Account creation (made via a Move, Add, Change (MAC) submission) should typically take NMCI between 1 and 5 business days once a correct and complete request has been officially submitted by the echelon 5 Navy Reserve Activity (NRA) Navy Operational Support Center (NAVOPSPTCEN), Squadron, etc. Upon NRA NMCI representative (i.e. CTR, Deputy Customer Technical Representatives (DCTR), ACTR) receipt of the account creation notification e-mail from NMCI, the total force member has 60 calendar days to meet in person (the member must be physically present) with a local registration authority (LRA) or trusted agent (TA) to have a token issued and associated to their new account. If the 60 days pass without token association, NMCI will automatically delete the account, and a new account must be requested. This will once again take approximately 1 to 5 business days to create.

c. Each echelon 5 and higher command must have at least three TAs per reference (p). The local TAs may request the SIPRNet token from the LRA after the individual requiring a token has received their SIPRNet account. The LRA will create the token and e-mail the personal identification number (PIN) (this is the number that enables the token to login into workstations)
to one of the TAs. The token will be mailed to a different TA (No single TA can hold both the pin and the tokens). The TA will ensure the token is provided to the user. An information system security manager (ISSM) or officer (ISSO) will be contacted by the command TA to have the account cryptographic logon (CLO) unenforced. CLO un-enforcement allows the user to logon to their SIPRNet account with just the username and password (this allows the opportunity to login and associate tokens to accounts). Once un-enforcement has occurred, the member must call NMCI to activate the account. After a new account has been associated to a token, Navy Reserve Force members must log in every 60 days to avoid account disablement, and every 90 to avoid deletion. If an account is locked due to user error (e.g. too many incorrect pin inputs) the member may call NMCI for restoration. If an account is disabled due to inactivity, an ISSM, or ISSO must call NMCI. If an account is deleted, the entire process must be repeated.

3. Account and Token Association

a. The Navy Reserve Force is a geographically dispersed, part-time force that can present challenges for echelon 5 NRAs to meet with total force members on a predictable schedule. As such, NMCI SIPR account finalization will require planning and coordination between supported commands, operational support officers (OSOs), echelon 4 Reserve Component Commands (RCCs), and echelon 5 NRAs to complete the actions above within the delineated time constraints.

b. Once a token is issued, the member will retain it while transitioning between commands and different network enclaves. Members will also retain their tokens until separation from the service. If a token is returned and is not damaged, it should be reused. Due to the minimum clearance requirements and a need to know, not all members receive tokens at accession. If a member did not receive a token from their accession command, and subsequently requires one for a SIPR account, then it will be the responsibility of the member’s supporting NRA or local Navy Reserve Force command to issue the token.

c. In order to support Navy Reserve member SIPR access, requirements need to be communicated from supported commands, via their designated OSO, to echelon 5 NRAs, and the identified total force member. It is the supported command OSOs responsibility to include these requirements in official orders (Active Duty Operational Support, recall, annual training (AT), or Active Duty for training (ADT)) and to ensure members have fulfilled those requirements prior to order execution. For Inactive Duty for training billets requiring SIPR accounts for performance of duties, supported command OSOs shall list the SIPR requirements in the job description in career management system interactive detailing (CMS-ID) for enlisted billets, or list them in the supported command comments in Reserve Force Manpower Tools (RFMT) for officer billets. NMCI SIPRNet account creation and token issuing/distribution will be the responsibility of the member’s supporting NRA or local COMNAVRESFOR command (i.e. If the member is not currently located at their assigned unit’s location). NRAs should have the capability to create NMCI SIPRNET accounts and associate SIPRNET tokens with them. COMNAVRESFORCOM (N6) can provide limited support to NRAs unable to provide NMCI
SIPRNet accounts and tokens onsite, including SIPRNet token association. Due to the restricted supply of tokens, COMNAVRESFORCOM cannot provide tokens for the entire Navy Reserve Force.

4. **System Authorization Access Request Forms.** SAAR-N forms are a prerequisite for access to any DoD system. Department of the Navy (DON) SAAR-N forms are referred to as SAAR-N forms (OPNAV 5239/14 (09-11)). SAAR-N forms sections 1-3 are required to be completed in full and kept on file by the local command.

5. **DEERS/RAPIDS (Other Accounts).** DEERS/RAPIDS workstations are considered Programs of Record (POR). They require direct connectivity to the building area network (BAN), local area network (LAN), or wide area network (WAN). The echelon 4 (i.e. RCC) COMNAVRESFORCOM (N6) staffs are responsible for placing the contract line item number (CLIN) X006AR-(Program of Record Wall Plug Upgrade or contract equivalent) on a task order via the NMCI ordering process. DEERS/RAPIDS terminals are controlled and maintained by Defense Manpower Data Center (DMDC); any issues with the system and its peripherals should be directed to the DMDC helpdesk at 1-800-372-7437. Issues such as the addition or removal of RAPIDS sites or the relocation of RAPIDS machines and equipment should be directed to the Navy Reserve Project office at navysupportprojectoffice@navy.mil COMNAVRESFORCOM (N1C4). Navy RAPIDS sites operated outside of NAVOPSPTCENs (i.e. Personnel Support Detachment (PSD)) should contact the Navy Project Office at (901) 874-4862.

6. **Government Furnished Equipment Phones, MobiKEY, and Mobile Cellular Data Device /Wi-Fi**

   a. **Smart Phones.** Smart phones/MCDDs requiring a data plan shall be authorized and ordered by COMNAVRESFORCOM (N63) against the authorized funding line. Smart phone users should have a mobile common access card (CAC) reader to send and receive encrypted e-mail and to digitally sign e-mail or documents.

   b. **Mobile Phones.** Stand-alone mobile phone services shall be procured through one of the Naval supply fleet logistics center (FLC) authorized vendors only, using the authorized funding line. They may not be purchased from retail stores or other non-FLC channels or funds. Stand-alone mobile phones may be purchased with voice and text services only. Data plans are not authorized.

   c. **MobiKEY**

      (1) Echelon 2, 3, 4, and 5 personnel who have a dedicated desktop may also be authorized a MobiKEY

      (2) Echelon 6 unit COs who have a dedicated desktop may choose a MobiKEY instead of a smart phone, or laptop with MCDD, or Wi-Fi card.
d. MCDD/Wi-Fi. The appropriate chief staff officer may authorize NMCI certified MCDDs for use with NMCI laptops. MCDDs can only be issued by COMNAVRESFORCOM N6 and are not authorized to be funded with local operating target (OPTAR) budgets.

7. **Message Traffic.** All commands will maintain their own Plain Language Address and the ability to transmit and receive message traffic (C2OIX) on both NIPRNET and SIPRNET.

8. **COMNAVRESFOR Customer Support Center**

a. The CSC provides support for all headquarter (HQ) IT requirements and asset management to include but not limited to: HQ on-site assistance, RC2/R2S specialized support services, Navy Message Traffic (COMNAVRESFOR, COMNAVRESFORCOM, COMNAVAIRFORES), teleconference/VTC/conferece scheduling and support, and Force wide support (as required that cannot be resolved at the command/RCC level.)

b. The CSC does not: Provide support for Navy E-Learning, Direct to Sailor (DTS), Navy Reserve Order Writing System (NROWS), NMCI related applications and programs, NMCI controlled assets, profile updates, NMCI accounts, RC2 e-mail forwarding, or assistance with personal devices.

9. **Very Important Person/Flag Officer IT Support**

a. In the event a Navy Reserve flag officer is in residence and requires assistance with NMCI related assets, the NMCI VIP Service is available at 1-877-274-8783.

b. The COMNAVRESFOR DCTR will procure, deploy, and provide equipment and customer service, to include follow-up on NMCI trouble tickets, to all flag officers attached to or working with any COMNAVRESFOR command, as required.

c. COMNAVRESFOR Flag VIP Program is ultimately managed by the COMNAVRESFORCOM Staff / DCTR personnel. Tasking and fielding of requests are handled by the designated Proxy(s) for each VIP which is set by the Authorized Proxy Management Tool in HP Service Manager.

d. Only the COMNAVRESFORCOM staff has permissions to set the proxy(s) for each individual Flag VIP. Request for changes/updates to respective proxy list should be requested via the NRH ticket portal.
CHAPTER 2

FACILITIES AND BUDGETARY GUIDELINES

1. **NIPRNET Assets.** All commands attached to COMNAVRESFOR shall adhere to the following updated baseline ordering model in order to meet NIPRNET computing and connectivity requirements. Direct all requests for explanation of this guidance to the COMNAVRESFORCOM NMCI Information Technology (IT) Operations Manager (N63).

   a. **Budget Guidelines.** COMNAVRESFORCOM manages the claimant-wide NMCI budget. Commands may make changes to their NMCI task order, but additions shall be authorized by COMNAVRESFORCOM (N63) to ensure the change remains within the authorized budget. All conditions of this instruction are dependent on the availability of funding.

   b. **Ordering Guidelines.** The ordering guidelines are a framework for assisting the RCCs in calculating the suggested asset allowance for each type of command in their area of responsibility. For the purpose of this subsection, Navy civilians and permanent contractors are considered FTS.

      (1) Echelon 2 through 5:

         (a) 1 NMCI seat for each FTS member.

         (b) NMCI training seat for SELRES as fiscal resources permit.

      (2) Commander, Naval Air Force Reserve Command Aviation Supply Departments (ASD)/Fleet Readiness Commands (FRC):

         (a) 1 NMCI seat for each FTS officer.

         (b) 2 NMCI seats for every 3 FTS enlisted.

         (c) NMCI training seat for 12 SELRES as fiscal resources permit ..

      (3) Navy Reserve echelon 6 Units:

         (a) 1 NMCI seat for the unit (CO).

         (b) 1 NMCI administrative seat. This seat can be either a portable or fixed seat.

         (c) Additional seats can be requested via the echelon 3 through 5 chain of command to support unit-specific requirements and/or mobilization readiness.
2. **SIPRNET Assets.** A minimum of one SIPRNET seat is authorized for each echelon 4 and 5 command. This requires a secure enclave. For more information pertaining to secure enclave requirements see Chapter 2 Space Certification and Chapter 3 KMI.

3. **Desktop Phones.** Ordering and repair processes and general responsibility for normal desktop phones reside with the host Service (i.e. U.S. Air Force Reserve), or Navy Installations Command (CNIC).

4. **Printing Services.** Per reference (a), COMNAVRESFORCOM is limiting the procurement of all networked and stand-alone DON pre-Next Generation Enterprise Network (NGEN) contract- procured Single-Function Devices (SFDs) copiers, printers, fax machines, scanners, Multi-Function Devices (MFDs), and related consumables and support services. This policy applies to all echelons of COMNAVRESFOR. COMNAVRESFORCOM (N6) has determined and the DON Chief Information Officer (CIO) has established the Defense Logistics Agency (DLA) as the single manager for printing and high-speed/high-volume duplicating, and the preferred provider of document conversion and automation services. Per reference (n), the Deputy Department of the Navy Chief Information Officer-Navy (DDCIO-N) has directed all echelon 2 commands to use DLA Services in alignment with DON CIO policy, as noted above. The overall objective is to achieve cost savings associated to consumables and maintenance at reduced cost. MFD implementation plan is as follows:

a. New requirements for office printing, scanning and photocopying of unclassified documents shall be met by purchasing an MFD. Detailed written guidance to assist with the leasing process associated with MFDs can be found on the COMNAVRESFORCOM (N63) CTR page on Navy Reserve Homeport.

b. New requirements for office printing, scanning, photocopying and faxing of classified documents shall NOT typically be met by use of MFDs.

c. Existing SFDs shall continue to operate until service life is met or a determination is made by the local command that the cost of supplies and maintenance would be greater than ordering a DLA MFD replacement.

d. SFDs that fail will be replaced by a DLA MFD as long as the procurement is within the bounds of the DLA assessment of the local command.

e. Should the DLA be unable to support a SFD request, consideration for purchase of a SFD shall have a DLA written waiver of approval to procure the device from another vendor. An Information Technology Procurement Request (ITPR) is required for the purchase of the new SFD and shall meet the requirements as set forth by the Chief of Naval Operations (CNO) as well as that which is required by the ITPR process. The SFD purchased, via a DLA printer waiver, shall also be listed on the NMCI Certified Device List. The waiver shall be attached to the ITPR and cannot be a network device. Reference (y) provides further detail.
f. SFDs in the same office work area as a DLA MFD shall be removed from service to the maximum extent practical to conserve resources. The MFD takes precedence over the SFD.

g. SFD copiers are on a separate DLA lease contract and can be operated until the cost/benefit of paying the DLA penalty fee for breaking the lease is more cost beneficial than having a MFD and a SFD copier on 2 separate contracts simultaneously. The MFD takes precedence over the SFD.

h. Unclassified MFD in SIPR space. MFDs are authorized for unclassified processing only. MFDs are authorized to operate within designated Open Secret Storage (OSS) areas without technical limitation. MFDs will display a “GREEN UNCLASSIFIED” label in plain sight of anyone operating the functions of the device. Local commands are responsible and accountable for all information processed on the MFD.

5. DEERS/RAPIDS Terminals. DEERS/RAPIDS terminals are controlled and maintained by DMDC and any issues with the system and its peripherals should be directed to the DMDC helpdesk at 1-800-372-7437. Issues such as the addition or removal of RAPIDS sites or the relocation of RAPIDS machines and equipment should be directed to the Navy Reserve Project Office at navyreserveprojectoffice@navy.mil (COMNAVRESFORCOM (N1C4)). Navy RAPIDS sites operated outside of NAVOPSPTCENs (i.e. PSD) should contact the Navy Project Office at (901) 874-4862.

6. Secure Space Certification

a. There are 2 different types of secure spaces that require certification in order to store, or use communications security (COMSEC) material within the Navy Reserve. Fixed COMSEC facilities and open storage spaces. The fixed COMSEC facilities require certification/re-certification through the Naval Communications Security Material System (NCMS) process using the immediate superior in command (ISIC) Inspector as the certifying official. Facilities must meet the requirements outlined in Electronic Key Management System (EKMS) 1(series) instructions for storage and processing of COMSEC material. Open Storage Spaces (OSS) are certified/re-certified by the CO or security manager must meet the requirements outlined in EKMS 1(series) and SECNAV M-5510.36 instructions. These types of spaces do not process or generate COMSEC material and should be treated and certified as such. With both types of spaces, the secure room (SR) checklist must be filled out by the local command hosting the facility and sent to COMNAVRESFORCOM (N6) KMI team. This checklist will be held in the command’s folder and utilized to generate the process of certification of the space to hold/process COMSEC material.

b. Once both types of spaces meet all requirements for certification, a designation letter will be generated either by the ISIC inspector in the case of fixed COMSEC facilities, or by the CO/security manager at the local command for OSS. This letter will be held (along with the SR checklist) both at the command in the secure space and by the COMNAVRESFORCOM (N6)
KMI Team. Until all conditions have been met the local command cannot hold/process COMSEC material within the space.

7. **Military Construction and Facility Restoration**

   a. **MILCON.** When a new Reserve Facility is approved through MILCON appropriations, it is the RCC’s responsibility to ensure that IT requirements are considered. Specific requirements should be vetted during the planning phase to ensure the new construction will adequately meet the needs of the Reserve Facility. The RCC shall track the progress of the new facility and order a site survey at the anticipated 80 percent completion date. Post site survey, the RCC shall submit a 6AG. RCCs shall keep COMNAVRESFORCOM (N63) apprised of any changes or delays.

   b. **NAVOPSPTCEN Rehabilitation.** When a Reserve Facility is approved through MILCON appropriations for rehabilitation, it is the RCC’s responsibility to ensure that IT requirements are considered. Specific requirements should be vetted during the planning phase to ensure the new construction will adequately meet the needs of the Reserve Facility. The RCC shall track the progress of the new facility and order a site survey at the anticipated 80 percent completion date. Post site survey, the RCC shall submit a 6AG. RCCs shall keep COMNAVRESFORCOM (N63) apprised of any changes or delays.
CHAPTER 3

MANAGEMENT RESPONSIBILITIES

1. **Introduction.** COMNAVRESFORCOM (N6) functions as the echelon 2 and echelon 3 IT department for COMNAVRESFOR. COMNAVRESFORCOM (N6) is responsible for the Force IT operations and Force IT budget execution. RCCs will be responsible for the administration of every COMNAVRESFOR command within their geographic region for all matters concerning Navy Reserve IT and related services, including NMCI. Exceptions are Office of the Chief of Navy Reserve Staff Detachment; Commander, Naval Information Force Reserve; Navy Air Facility Washington; Navy Air Logistics Office and Navy Reserve Professional Development Center will be responsible for managing NMCI in their cognizant areas within COMNAVRESFOR.

2. **System Change Requests**

   a. IT change requests may be submitted to COMNAVRESFORCOM (N6) via the procedures defined in the COMNAVRESFORCOM (N6) configuration management plan located on the Navy Reserve Homeport N6 page at the following location: https://private.navyreserve.navy.mil/cnrfc/N-Codes/N6. IT change requests will fall into 1 of 2 categories; enhancements to current capabilities or new requirements. Enhancements will encompass proposed upgrades to the COMNAVRESFOR IT enterprise including processes, hardware, software, and documentation. New requirements include requests for digital capabilities and solutions, features, functionality, documentation, hardware, or software that are not currently in the COMNAVRESFOR IT enterprise.

   b. The COMNAVRESFORCOM (N6) IT Configuration Control Board (CCB) is the official mechanism for controlling changes to the configuration baseline of the COMNAVRESFOR IT enterprise, and it is the governing body chartered to ascertain all impacts of proposed changes. The CCB provides necessary prioritization for all significant IT change requests as well as executive oversight for change management. The CCB also ensures that changes are made in a controlled manner and are documented in the operational architecture. All COMNAVRESFOR commands and activities shall utilize the COMNAVRESFORCOM (N6) IT CCB as the authoritative source for COMNAVRESFOR IT enterprise configuration changes. The CCB will be tasked to review, approve, and prioritize incoming IT change requests. The COMNAVRESFORCOM (N6) configuration manager will determine which requests are routed to the CCB via the local CCB. Meetings will include the request originator and COMNAVRESFOR stakeholders as needed to ensure that the interests of their respective organization(s) are represented. The COMNAVRESFORCOM (N6) IT CCB is established to serve the following purposes:

   (1) Represent the interests of all groups who may be affected by changes to the baselines.
COMNAVRESFORINST 5300.5B
12 Feb 2019

(2) Authorize the creation of products from the baseline library of the COMNAVRESFOR IT enterprise.

(3) Evaluate and approve or disapprove proposed changes to controlled configuration items.

(4) Prioritize approved changes.

3. **IT Inventory.** Inventory of NMCI NIPRNET/SIPRNET assets, such as NMCI desktop computers and laptops, and other IT assets, such as MFDs, MCDDs, MobiKEYs, Wi-Fi cards, GFE cell phones and smart phones, and software licenses, will be required of the RCCs, in conjunction with their subordinate commands, on an annual basis, at each change of command, or as scheduled by COMNAVRESFORCOM. Corrections to errors will be made in the NET as the sole authority on that data. RCC personnel completing IT inventories and working with NET are to complete NET training via the CTR training page on the NMCI Homeport.

4. **NMCI Pre-Invoices.** The DCTR shall ensure NMCI pre-invoices are validated as required, utilizing eMarketplace.

5. **Non-NMCI IT Procurement Requests.** All non-NMCI IT purchases, regardless of cost, are required to be submitted and an approved ITPR via the Navy Information Technology Approval System (NAV-ITAS), see reference (y) for further details.

6. **NMCI Services request (6AG)/RAPT infrastructure:**

   a. **RAPT** is a Contracts application which documents the requirement approval and PCO (Procurement Contracting Office) acquisition process and serves as the NMCI electronic contract file. Typically, CLIN 6AG’s are used to make changes to the NMCI infrastructure. This can be as simple as adding a new blade to an existing switch; to a more complex project such as establishment and wiring a new building. 6AG’s can also be used to install new wall drops in conjunction with a switch installation for easier project management. The 6AG process is started by procuring a survey and a travel CLIN (if required), and submitting the 6AG survey form which will result in a working rate card (WRC). Once the WRC is received by the command they will open a 6AG RAPT request, which will result in the award of CLIN’s for the project. The command must order the CLIN’s for the vendor to start the work.

   b. Contact your CTR for assistance in creating a 6AG RAPT Request. The purpose of the RAPT Request is to automate the approval and negotiation processes for unpriced requests and general contracting actions. The tool is created around basic workflow functionality where CTRs create requests by completing questionnaires that are then routed through an approval process. The RAPT process consists of requirements generation, claimant approval, technical evaluation, price analysis, contract negotiation, and award. The tool provides a repository of approved, rejected requests, and corresponding document repository as a record. CLINs (or
contract equivalent) are created as a result of an awarded request and are written to NET, where they are enabled for ordering.

c. The 6AG process is started by procuring a survey and a travel CLIN (or contract equivalent, if required), and submitting the 6AG (or contract equivalent) survey form which will result in a working rate card (WRC). The command will open a 6AG RAPT (or contract equivalent) request upon receipt of the WRC. Submission of the RAPT request will result in award of orderable CLINs (or contract equivalent) for the project. The command must order the CLINs (or contract equivalent) for the vendor to start the work.

7. Account management, ISSM/ISSO responsibilities, LRA, TA

a. ISSM (echelon 2/echelon 3) responsibilities:

(1) Ensure that all cybersecurity components have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an Information system (IS) or Platform Information Technology (PIT) system.

(2) Be trained, qualified, and appointed in writing by the commanders of DON organizations. Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives, policies, cybersecurity personnel, cybersecurity processes, and procedures.

(3) Maintain a repository for all organizational or system-level cybersecurity-related documentation.

(4) Ensure that ISSOs are appointed in writing and provide oversight to ensure that they are following established cybersecurity policies and procedures.

(5) Monitor compliance with cybersecurity policy, and review the results of such monitoring.

(6) Ensure that cybersecurity inspections, tests, reviews are scheduled, synchronized, and coordinated with affected parties and organizations.

(7) Ensure implementation of IS security measures, procedures, including reporting incidents to the commander, command security manager, appropriate reporting chains, and coordinating system-level responses to unauthorized disclosures in accordance with applicable DoD instructions, directives, and notices.

(8) Periodically assesses the quality of security controls implementation against performance indicators, such as: security incidents; feedback from external inspection agencies
b. ISSO (echelon 4) responsibilities:

(1) ISSO serves as the principal advisor to the ISSM on all matters, technical, and otherwise, involving the security of an information system. The ISSO typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many cases, is assigned responsibility for the day to day security operations of the system.

(2) This responsibility may also include, but is not limited to, physical security, personnel security, incident handling, and security awareness and training. The ISSO may be called upon to assist in the development of the system security policy and to ensure compliance with the policy on a routine basis.

c. LRA responsibilities:

(1) The LRA's primary responsibility is to properly register users in the PKI system, so that users can obtain PKI certificates. This involves verifying a user's identity and entering the user's information in a special LRA application on the LRA's workstation. LRAs do not need to directly manage or keep track of user keys and certificates; however there are occasions when a user's certificate must be revoked, and/or a new certificate for the user is required. The LRA provides support in these circumstances.

(2) Informing users of their responsibilities (DD-Form 2842 (08-09)).

(3) Assisting users with the management of keys and certificates.

(4) Managing a central workstation for registration (if the site requires one).

d. TA responsibilities:

(1) A TA is an individual who supports an LRA by performing the face-to-face user authentication and handing out the Certificate Registration Instruction (CRI) forms for the LRA. The trusted agent concept allows easier registration of users at remote locations, where it may be impractical for the user to come in person to an LRA or vice versa.

(2) Validation that the subscriber is eligible to be registered (U.S. Military, DoD civilian, contractor, or others using government furnished equipment and working in government spaces).

(3) Gathering and forwarding subscriber registration information to the LRA.
(4) Delivering certificate CRI and initialized tokens or keyed tokens and/or activation data to subscribers.

(5) Verifying the identity of each subscriber as specified in Section 3.2.3 of the DoD Registration Practice Statement (RPS).

(6) Assist subscribers in the downloading and installation of their certificates.

(7) Reporting to the LRA if a subscriber suspects a compromise or loss of a private key.

8. **SAAR-N forms.** SAAR-N forms are a prerequisite for access to any DON system. SAAR-N forms sections 1-3 are required to be completed in full, and kept on file by the local command. A favorable National Agency Check with Local Agency Checks and Credit Check (NACLC) is required for unclassified network access. For military members, in most cases network access may be granted if the NACLC is expired. For military, government employees, and contractors, in instances where no NACLC was ever started, the NACLC shall be initiated before permitting unclassified network access to personnel. If personnel have a revoked or denied NACLC status, the issues shall be resolved within 2 years at the individual’s current command or network access should be restricted. SAAR-N section 4 will be completed as required. Commands shall retain SAAR-N forms for 6 years after user account is terminated or when no longer needed for investigatory or security purposes, whichever is later.

9. **KMI.** KMI formerly EKMS, is designed to provide communications security (COMSEC). Examples include Tactical Local Area Network Encryption (TACLANES), Secret Telephone Equipment (STE), and more.

   a. SIPRNET capability is for secure internal Reserve Force communications only. COMNAVRESFOR is not funded for additional SIPR seats to support gaining commands. However, if an NRA wants to add SIPR seats, it may do so provided it can obtain one or more of the following:

      (1) Gets COMNAVRESFORCOM (N6) authorization.

      (2) Have sufficient room in its secure enclave for additional drops and seats.

      (3) Have sufficient space available on the switch.

      (4) If in support of a gaining command, obtain funding from the gaining command.

   b. COMNAVRESFOR commands will maintain SIPRNET capability. All sites require 24/7 access to SIPRNET and STE. If a command does not have on-site access, then steps shall be taken to meet SIPR requirements. If a site is unable to meet these requirements, but has the ability to procure access via another acceptable DoD facility, requirements can be satisfied with a
Memorandum of Agreement (MOA). COMNAVRESFOR does not support removal of SIPRNET at sites in either of the following conditions:

(1) The CO would prefer to leverage a MOA with a nearby DoD facility.

(2) The CO does not want the responsibility of operating a SIPRNET computer or STE.

c. COMNAVRESFORCOM is the KMI parent account (for many of its subordinate commands referred to as Local Elements (LEs)). If a command possesses COMSEC material provided by COMNAVRESFORCOM (TACLANEs, STEs, etc.) a Memorandum of Understanding (MOU) will be signed in black ink by the LE CO and COMNAVRESFORCOM Staff Security Material System Responsibility Officer (SCMSRO). The CO has ultimate responsibility for conduct of the KMI LE account.

(1) The MOU is a formal agreement between the LE and COMNAVRESFORCOM outlining proper COMSEC responsibilities.

(2) All LEs are required to have at least 2 custodians (the CO cannot be one of the two). These members will administer the equipment/material. They will be formally qualified upon completion of training provided directly by the COMNAVRESFORCOM KMI team.

(3) Change of command responsibilities. A 30 day notice will be provided to the COMNAVRESFORCOM KMI team to ensure an inventory is completed and new MOU signed.

(4) Semi-Annual inventory. All LEs will provide inventories (SF 153) for their accountable material to the COMNAVRESFORCOM KMI team every February and August.

(5) Annual rekey. All LEs are required to turn in TACLANEs each year to the COMNAVRESFORCOM KMI team for rekey. STEs must also be updated. This must be completed each year by the end of April. Guidance will be provided annually for the evolution.

(6) LEs are required to provide connectivity updates via SIPR e-mails and STE calls, participate in monthly training, and conduct quarterly spot checks, amongst other set requirements delineated in each MOU, EKMS 1 series literature, and COMNAVRESFORCOM KMI team guidance.


a. Landing Page, considered to be the first viewable page for each command. Each section of the landing page shall adhere to the COMNAVRESFOR approved layout. This page will contain:

(1) Command name
(2) Mission statement

(3) Easy tab section 1

(4) Leadership section with photos and biography links

(5) Plan of the month

(6) Drill schedule

(7) Staff directory

(8) Command profile (address, hours of operation, contact phone numbers, command logo)

(9) Easy tab section 2

(10) Announcements

(11) Command calendar

(12) Hyperlinks to site owner to a valid and official Navy e-mail address

(13) Command Interactive Customer Evaluation link (ICE) must be hyperlinked to a valid ICE comment card

(14) COMNAVRESFOR maintained required awareness logos (i.e., Sexual Assault Prevention and Response, Anti-Terrorism/Force Protection, Suicide Prevention)

(15) SAPR POC: must contain three points of contact information. Local contact information from the command must be used unless unavailable. Regional contact information may be used in the event that local representatives are not present

(16) Additional site pages are authorized as required by each command

b. Creation of sub sites for lower echelon commands requires the completion and submission of a site request form located at https://private.navyyreserve.navy.mil/coi/SPTC/Pages/default.aspx site request must be sent to the RCC for approval and forwarded from the RCC to COMNAVRESFOR helpdesk via the CSC Ticketing system. Sites created by personnel other than COMNAVRESFORCOM (N6) personnel are not authorized and may be subject to deletion.
(1) RCCs shall monitor and validate site standardization for lower echelon commands. All sites and subsite standardization shall be tracked via the NRH Standardization tracker located: https://private.navyreserve.navy.mil/cnrfc/N-Codes/N6/sharedservices/Pages/NRH-Standardization.aspx

c. Site troubleshooting. Troubleshooting SharePoint related items should be handled at the lowest echelon level, as required using the IT chain of command.

d. Site permission management. To verify each person is assigned appropriate privileges/permissions, each command will validate its subordinate command’s assignments to site owner roles. Example: RCCs will validate NAVOPSPTCENs; NAVOPSPTCENs will validate Reserve Units. The permission level “full control” will be limited to COMNAVRESFORCOM (N6) personnel.

(1) Community of Interest site permissions (full control) will be approved and maintained by submitting a ticket to COMNAVRESFOR’s helpdesk. Submitted tickets shall include parent site URL, for which permissions are being requested.

(2) Other permissions will be maintained by local SharePoint site owners but maybe validated at any time by the RCC or COMNAVRESFORCOM (N6) personnel.

e. SharePoint training. Review of SharePoint training powerpoint presentations are required by all personnel prior to receiving permissions to author, manage, or contribute site information.

(1) SharePoint site owners are required to review SharePoint training levels 100, 200, and Site Owner PowerPoint presentations prior to receiving “Full” permissions. Training presentations are located on the (N6) SharePoint page.

(2) Contributors are required to complete SharePoint training level 100 prior to receiving contribute permissions.

(3) COMNAVRESFORCOM (N6) will schedule additional SharePoint training monthly and on a requested basis.

f. User profile synchronization. All military, government civilian, or contractor personnel requiring access to SharePoint shall have a .mil or .gov e-mail address associated to his or her profile.

(1) SharePoint user profiles (display name, phone number, e-mail address) will automatically update via the user profile synchronization for users who maintain an NMCI e-mail account.
(2) Non-NMCI users will be required to contact COMNAVRESFOR’s sharepoint helpdesk for manual updates to their SharePoint User Profile (display name, phone number, e-mail address).

g. Linking “.COM” Websites. Linking of “.COM” websites/links will be allowed on SharePoint pages only if they have a mission need and those sites have been screened/reviewed for associated risks by COMNAVRESFORCOM (N64).

h. Posting of official Navy documents or information to non-Federal Risk and Authorization Management Program (FEDRAMP) rated Cloud services or Cloud services that do not meet minimum Cloud security requirements as stated in reference DON CIO Memo: Acquisition and Use of commercial cloud computing services, such as Google Drive, Dropbox or Box is prohibited. Documents approved for “official public release” by the Force PAO or PAO representative are exempt.

11. Collaboration Tool: Defense Collaboration Services. Navy-wide ashore use of DCS will be the standard collaboration tool for chat and web conferencing. DCS is the single designated and approved enterprise tool for NIPRNET and SIPRNET web-based conferencing, instant messaging, “white boarding” and application sharing.

   a. All users with online collaboration responsibilities will obtain DCS accounts and maximize use of DCS capabilities. Users shall have a CAC in order to register for an account.

   b. Waiver requests for alternate collaboration tools are required for commands that are unable to comply with the DCS requirement and these waivers shall ultimately be approved by the DDCIO-N via COMNAVRESFOR.

12. NNWF Usage Procedures and User Responsibilities

   a. These procedures will include, but are not limited to, mandatory wireless device set-up requirements for maximum cybersecurity, security, and overall user responsibilities. Only those wireless devices meeting the standards specified in this instruction are approved for connectivity to NNWF. The procedures and policy items contained within this document meet the requirements of reference (k).

   b. These procedures and user responsibilities apply to all COMNAVRESFOR military, civilian and contract personnel assigned to locations with NNWF services installed, system maintainers and managers, all users, and all wireless infrastructure devices connecting to the Wi-Fi network. User access to NNWF resources is a privilege. Responsible system management is required to maintain confidentiality, integrity and availability of information assets.

   c. Responsibilities
(1) NNWF Program Manager shall:

   (a) Provide NNWF program management and overall risk management.

   (b) Coordinate with COMNAVRESFOR ISSM to adjudicate cybersecurity violations related to NNWF usage and make recommendations for all cases.

(2) RCC (N6) shall:

   (a) Report all cybersecurity violations to COMNAVRESFOR ISSM and assist in all administrative matters pertaining to NNWF.

   (b) Conduct periodic site visits to inspect and ensure adherence to COMNAVRESFOR cybersecurity requirements. Inspections will include, but are not limited to: User registration process, router pass-phrase management process, physical security of NNWF equipment, user conduct in NNWF spaces and signal footprint, to ensure broadcast does not bleed into classified spaces.

   (c) Maintain situation awareness regarding NNWF use at subordinate commands.

   (d) Make recommendations to COMNAVRESFOR to install new NNWF networks at COMNAVRESFOR sites with a high demand signal for network usage or to add Wireless Access Points (WAP) to current site configurations.

(3) NAVOPSPTCEN COs/officers-in-charge (OICs) shall:

   (a) Implement and ensure adherence to this policy. CO/OIC’s direct involvement is required to ensure that security and cybersecurity is maintained.

   (b) Enforce strict compliance with NNWF usage policy and ensure access is denied to users who violate policy.

   (c) Verify physical security of NNWF system router in a secure, locked space. Do not permit tampering with system settings.

   (d) Make recommendations to echelon 4 to install NNWF at COMNAVRESFOR sites with a high demand signal for network usage or to add Wireless Access Points (WAP) to current site configurations.

(4) NAVOPSPTCEN/COMNAVRESFOR site ISSM/ information systems security officer (ISSO) shall:
(a) Act as designated administrator of the NNWF network, and take responsibility for implementation of procedures for validating users and wireless devices.

(b) Ensure WAP pass phrase is strong. The pass phrase shall be a of minimum 14 characters, including 2 upper case, 2 special and 2 numeric characters. Pass phrases shall be changed at least once every 60 days. NMCI laptops are authorized for changing WAP pass phrases. COs should take steps to ensure minimal service disruption during this time.

(c) Verify all wireless devices are configured for maximum security. The COMNAVRESFOR (N63) portal verification will be utilized to completed verifications prior to connection to the NNWF network.

(d) Ensure all NNWF users have completed cybersecurity, personally identifiable information (PII), and operations security (OPSEC) annual training. If delinquent, users shall not be permitted to connect to NNWF.

(e) Ensure users requesting access to the NNWF network complete the NNWF User Agreement-SD Form 815 (03-97), Wi-Fi user agreement. SD Form 815 (03-97) will be reviewed annually and be retained for 2 years from the approval of access.

(f) Maintain oversight of the user registration form on the SharePoint Reserve Force Wi-Fi portal that maintains individual user account information to include the MAC address of each user’s personal computer. Verify that each user has completed the registration form in its entirety.

(g) On the initial device connection to the NNWF network, verify that each user has the latest version of anti-virus protection software on his or her personal computer. A link to a web site for anti-virus software download is available on the COMNAVRESFORCOM (N64) portal.

(h) If any user is found to be in violation of this instruction or cybersecurity procedures, immediately report user to the NAVOPSPTCEN CO/unit OIC and block the respective device’s MAC address at the router.

(i) Conduct random walk-through inspections in wireless internet capable spaces to verify proper use. Report misuse to the NAVOPSPTCEN CO/unit OIC and ensure the user disconnects his or her computer from the NNWF network.

(j) Due to specific security requirements for NNWF, ensure physical integrity of the router and its installed parameters. The router shall remain in a locked and secure space. Settings shall not be modified once installed.

(k) Maintain a copy of “Century Link Post-Implementation Support Process
Procedures,” available via echelon 4 and follow procedures to address any technical issues.

(5) NNWF Users shall:

(a) Follow the procedures and policy set forth in this instruction and the NNWF User Agreement.

(b) Ensure personal computing devices have requisite hardware installed, including a wireless adapter and CAC reader.

(c) To expedite access to NNWF resources, ensure personal computing device meets the requirements of the NNWF User Agreement prior to drill weekend or first use of NNWF network, and completed cybersecurity, personally identifiable information (PII), and operations security (OPSEC) annual training.

(d) Complete NNWF User Agreement, via the link found on the COMNAVRESFOR Wi-Fi portal within the private CAC-enabled SharePoint portal. Access to NNWF is strictly dependent on users having a current SAAR-N on record, and completing the user agreement form linked to this registration process.

(e) Use NNWF to connect to .mil, .gov, .edu domains, and other authorized internet sites, as set forth in the DON IT Acceptable Use Policy. NNWF is only to be utilized for accessing public-facing websites and DoD public-facing CAC-enabled websites.

(f) Ensure no sensitive information, including documents containing PII or For Official Use Only (FOUO) information, are stored on personal computing devices, including personal hard drives, computer memory, and temporary files.

d. Troubleshooting Personal Devices. The NAVOPSPTCEN CO, site OIC, or local ISSM/ISSO or Cybersecurity Workforce (CSWF) personnel are prohibited from troubleshooting personal computing devices. The vast number of operating systems and hardware configurations loaded on personal computers make this function beyond the scope of CSWF personnel.

(1) Troubleshooting systems is a personal responsibility.

(2) Users bear all risk associated with the use of NNWF network. The government is not liable for any damage or loss incurred as a result of network use.

e. Enforcement. A user found to have violated this policy will have their NNWF privileges revoked and may be subject to disciplinary action. Users may be reinstated at the direction of the COMNAVRESFOR ISSM. The level of reinstating authority depends on the nature and scope of the violation. Example violations warranting access denial include:
(1) Improper use of NNWF, as defined in the user agreement.

(2) Visiting sites that would bring discredit to Naval Service (e.g. gambling sites, pornography).

(3) User does not have a current NMCI account.

(4) User is deficient in annual cybersecurity, PII, or OPSEC training.

(5) Other reasons as determined by site commander, RCC, echelon 4 ISSM, or COMNAVRESFOR ISSM.

13. Cyber Security Workforce CSWF.

a. In accordance with DON and DoD requirements, commands must establish and manage a Cyber Security Workforce (CSWF) program to staff, train, and sustain a professional IT workforce with a common understanding of Cyber Security (CS) concepts and principles, and the skills needed to effectively prevent and respond to attacks against government information systems and networks.

b. The cyber IT/CSWF will be composed of those individuals who perform cybersecurity functions. This includes personnel who secure, defend and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities. It also includes personnel who design, build, configure, operate and maintain IT, networks and capabilities. This includes actions to prioritize portfolio investments, architect, and engineer, acquire, implement, evaluate, and dispose of IT and services; as well as information resources management, management, storage, transmission, and display of data and information.

c. Commands will assign at least one cyber IT/CSWF-PM (appointed by CO) to track and manage their local CSWF program. Military and Government personnel filling cyber IT/CSWF positions shall obtain the appropriate DON-approved baseline job qualification standards within 6 months of assignment. The CO will ensure that military and civilian personnel are appropriately qualified. CSWF members will maintain eligibility by completing annual continuing education (CEU) requirements, and ensuring annual maintenance fees are paid on time per credentialing agencies’ policies. CSWF members are responsible for tracking their CEUs and maintenance fee status, and ensuring they submit vouchers to the USN Certification Funding program: Navy Credentialing Opportunities On-Line (Navy COOL) (www.cool.navy.mil) via command ISSM. Navy COOL will fund initial certification exams and annual maintenance fees. Navy COOL does not fund training, study prep materials, memberships, or other non-exam fees.
d. Supervisors will ensure civilian CSWF members develop an Individual Development Plan (IDP) to identify planned educational opportunities and courses they will complete to meet training and CEU requirements. IDP will be created and stored in Total Workforce Management System (TWMS) IDP module by civilian CSWF members, and sent to supervisors for review and approval. Supervisors will ensure members are on track with training requirements throughout the year, and report status to COMNAVRESFORCOM CSWF-PM quarterly.

(1) Earn and maintain appropriate credentials from the cyber IT/CSWF qualification matrix (described in SECNAV M-5239.2) associated with the specialty area and level commensurate with the scope of major assigned duties for the position to which you are assigned.

(2) Participate in a continuous learning program as described in SECNAVINST 1543.2. A minimum of 40 hours of cyber IT/CSWF related continuous learning annually documented in a current individual development plan.

(3) Uniformed CSWF personnel remain part of the CSWF regardless of whether they are currently assigned to a CSWF position. Civilian personnel are considered part of the CSWF when assigned to a CSWF position. CSWF personnel may be identified in the following ways:

(a) A DON CSWF code and/or DoD function is part of their personnel record in a military personnel system or in Defense Civilian Personnel Data System (DCPDS).

(b) An identified military code such as Military Occupation Specialty (MOS), Navy Enlisted Code (NEC), Sub Specialty Code (SSC), or Additional Qualification Designator (AQD). They are listed as a member of the CSWF with the appropriate DON CSWF code in the DON/Navy/Marine Corps authoritative personnel and readiness databases. Expected participants include: Government Civilians (2200 series), and/or those performing duties as described in SECNAV M-5239.2 Military enlisted (Information Technology Specialist), or other ratings performing duties as described in SECNAV M-5239.2 Military Officers performing duties as described in SECNAV M-5239.2.

e. Cyber IT/CSWF personnel training and qualification compliance shall be monitored by the cyber IT/CSWF-PM. COs shall assign unqualified military and civilian personnel to a supervised status for qualification/requalification or remove unqualified personnel from their cyber IT/CSWF position while requalification is completed. Those who fail to requalify shall be permanently removed from the cyber IT/CSWF. In addition to removal from cybersecurity positions, failure to maintain required qualifications will result in counseling and proper documentation by the cyber IT/CSWF-PM and chain of command.

14. User Training. In order to access DON Information Systems, users must complete annual cybersecurity awareness, PII, and OPSEC awareness training annually. Users that do not complete
these annual requirements to meet DoD and DON guidelines each fiscal year shall have their account disabled. More information can be obtained in COMNAVRESFORINST 5239.3A.

15. **Continuity of Operations Plan.** COMNAVRESFOR will verify functionality of the COMNAVRESFOR IT Continuity of Operations Plan (COOP) by exercising the COOP annually as required by reference (h). COOP dates will be advertised for command planning purposes.

   a. Upon completion of the annual exercise or actual COOP, all commands are required to validate their site content for access and functionality.

   b. RCC N6s shall notify all NAVOPSPTCEN leadership, and N6 personnel when COMNAVRESFOR is implementing its COOP, whether during COOP-related exercises, or an actual real-life scenario in which COOP would be implemented. This will ensure situational awareness of potentially degraded services from higher echelons.

16. **DEERS/RAPIDS.** Workstations require direct connectivity to the Building Area Network (BAN) / Local Area Network (LAN) / Wide Area Network (WAN). The regions (RCC-echelon 4) N6 staffs are responsible for placing the CLIN X006AR-(Program of Record Wall Plug Upgrade) on a task order via the NMCI Contract process. DEERS/RAPIDS terminals are controlled and maintained by DMDC and any issues with the system and its peripherals should be directed to the DMDC helpdesk at 1-800-372-7437. Issues such as the addition or removal of RAPIDS sites or the relocation of RAPIDS machines and equipment should be directed to the Navy Reserve Project Office at navyreserveprojectoffice@navy.mil (COMNAVRESFORCOMN1C4). Navy RAPIDS sites operated outside of NAVOPSPTCENs (i.e. PSD) should contact the Navy Project Office at (901) 874-4862.

17. **Outlook Web Access.** Access to NMCI’s Outlook Web Access (OWA) unclassified official e-mail using personally owned and other non-DoD computers is authorized provided Commanders and users adhere to the procedures in the acceptable use of DON IT memorandum located on the Navy Reserve Homeport N6 page.

18. **CAC Readers (non-R2S).** CAC readers are considered consumables that can be purchased by each echelon’s Supply department (N4), subject to the funding availability.
Appendix A

ACRONYMS AND DEFINITIONS

The following is a list of the current acronyms and definitions referenced throughout this instruction.

**Anti-Virus Software.** Software designed to prevent, detect and remove malware, including but not limited to computer viruses, computer worms, Trojan Horses, spyware, and ad-ware.

**Authority to Operate.** An Authority To Operate (ATO) is the formal approval (accreditation) to operate a system, which is granted by the DAA. Once granted, an ATO is good for three years.

**Common Access Card (CAC).** A U.S. DoD issued smart card for multifactor authentication to networks and information systems. CACs are issued as standard identification for Active-Duty military personnel, Reserve personnel, civilian employees, non-DoD government employees, state employees of the National Guard and eligible contractor personnel. In addition to its use as an identification card, a CAC is required for access to government buildings and computer networks.

**CAC Reader.** A physical device used as a communications medium between the CAC and a host (e.g., a computer, a point of sale terminal) or a mobile phone.

**Media Access Control Address.** A unique identifier assigned to network interfaces and devices for communications on the physical network segment.

**Office of the Designated Approving Authority (DAA).** Provides centralized management and decentralized execution of the Certification and Accreditation (C&A) process for all DoD information systems. The Office of the DAA is accountable for timely, consistent policy implementation and C&A determinations with the DoD.

**Pass Phrase.** A sequence of words or other text used to control access to a computer system, program or data. A pass phrase is similar to a password in usage, but is generally longer for added security.

**Personally Identifiable Information.** Refers to information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a single individual. This includes name, birth dates, Social Security Numbers, rank, address, phone number, etc.

**Physical Security.** Describes measures designed to deny access to unauthorized personnel (including attackers, or even accidental intruders) from physically accessing a building, facility, resource or stored information.

**Wi-Fi.** A branded standard for wirelessly connecting electronic devices. A Wi-Fi device, such as a personal computer, can connect to the internet via a wireless network access point.
Appendix B

NAVY RESERVE FORCE (NAVRESFOR) NAVY OPERATIONAL SUPPORT CENTER (NAVOPSPTCEN) WI-FI (NNWF) USER DEVICE INITIAL SET-UP CHECKLIST

1. Before initially being approved for connecting to the NNWF Network, the following actions shall be completed:
   a. Verify Cybersecurity, PII, and OPSEC (as required) annual training requirements are within periodicity.
   b. Register as a new user to the NNWF network on the NNWF website, accessible by link on NRH Private Portal, COMNAVRESFORCOM, N6 homepage. Ensure your MAC address and drill site location is captured and accurate.
   c. Sign and date NNWF User Agreement form.
   d. Install and test CAC reader on the personal laptop.
   e. Ensure user has updated anti-virus software installed.
   f. Enable firewall.
   g. Print confirmation of registration.
   h. Receive pass phrase from designated command ISSM/ISSO or applicable CSWF personnel.

2. After initial approval for NNWF access is granted, users are responsible for maintaining virus updates and ensuring the firewall is enabled prior to network access per the User Agreement.
Appendix C

REFERENCES

(a) CIO memo of 25 Jan 13 MFD Guidance
(b) DoD 5500.07-R, Joint Ethics Regulation, November 2011
(c) SECNAV 192027Z Aug 10
(d) SECNAV 192031Z Aug 10
(e) SECNAVINST 5239.3B
(f) SECNAVINST 5210.8E
(g) DON CIO 032009Z Oct 08
(h) 44 U.S.C. § 3541
(i) SECNAV M-5510.30, Department of the Navy Personnel Security Program
(j) SECNAV M-5210.1, Rev. 1, Records Management Manual
(k) COMNAVNETWARCOM Itr 5239 Ser ODAA/1001 of 9 May 11
(l) DON CIO 161108Z Jul 05
(m) DoD Instruction 8500.2 of 6 February 03
(n) DDCIO (N) memorandum of 17 Sep 13
(o) DSECDEF memo 15 Jan 18, Conducting Official Business on Electronic Messaging Accounts
(p) CNO Washington DC 121935Z Mar 12 (NAVADMIN 084/12) Router Network
(q) EKMS-1E Electronic Key Management System (EKMS) Policy and Procedures for Navy Tiers 2 and 3
(r) SECNAV M-5510.36 Department of the Navy Information Security Program
(s) Acceptable Use of Department of the Navy (DON) Information Technology (IT) Memo 12 February 2016
(t) DoD Registration Practice Statement
(u) SECNAV M-5239.2
(v) DoD Directive 8140
(w) SECNAVINST 1543.2
(y) CNO Washington DC 201202Z Sep 17